

REMARKS / DISCUSSION OF ISSUES

The present amendment is submitted in response to the Office Action mailed September 27, 2010. Claims 1-12 remain in this application. Claims 1-3 and 5-21 have been amended. Claim 4 has been cancelled. In view of the amendments above and remarks to follow, reconsideration and allowance of this application are respectfully requested.

Interview Summary

Applicants appreciate the courtesy granted to Applicant's attorney, Michael A. Scaturro (Reg. No. 51,356), during a telephonic interview conducted on Wednesday, May 11, 2011. During the telephonic interview, discussion turned to the novelty of the invention. Applicant's Attorney provided reasons why the proposed amendment to claim 1 overcomes the presently cited and applied art. The Examiner appreciated the explanation and will consider the arguments when presented in Applicant's response.

Claim Rejections under 35 USC 103

- I. In the Office Action, Claims 1, 2 and 4 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,013,391 ("Herle") in view of U.S. Patent Publication No. 20030211842 ("Kempf"). Applicants respectfully traverse the rejections.

Claim 1 is allowable

Independent Claim 1 has been amended herein to better define Applicant's invention over the combination of Herle and Kempf. Claim 1 now recites limitations and/or features which are not disclosed by Herle or Kempf, taken alone and in any reasonable combination. Therefore, the cited portions of Herle and Kempf do not anticipate claim 1, because the cited portions of Herle and Kempf do not teach every element of claim 1. Claim 1 is reproduced below in clean form.

1. (Currently Amended) A method of distributing the location of a mobile device comprising the steps of:
 - the mobile device determining its location;
 - the mobile device encrypting the determined location using a predetermined encryption key; and
 - the mobile device uploading the determined encrypted location and a telephone number of the mobile device to a server for storage as a database record associated with the mobile device;
 - the server storing the received encrypted location of the mobile device in the database record associated with the mobile device;
 - the mobile device communicating with a remote terminal, including sharing the predetermined encryption key with the remote terminal by attaching the encryption key to the communication, wherein the encryption key is not shared with the server; and
 - the remote terminal querying the database supported by the server by sending the telephone number of the mobile device in response to receiving the communication from the mobile device;
 - the server transmitting to the remote terminal the encrypted location of the mobile device in response to the query;
 - the remote terminal decrypting the encrypted location of the mobile device using the predetermined encryption key received from the mobile device.

Claim 1 now more clearly and precisely describes a method of distributing the location of the mobile device which safeguards the privacy of the user of the mobile device.

In applicant's specification, there is described an example scenario in which a user in possession of a telephone MS1 (claim 1 - remote terminal), receives a text message (communication) from a friend, the user of telephone MS2 (claim 1 - mobile device). Appended to that text message is an encryption key (claim 1 – predetermined encryption key). The aforementioned steps are recited as the following element of claim 1:

.... the mobile device communicating with a remote terminal, including sharing the predetermined encryption key with the remote terminal by attaching the encryption key to the communication, wherein the encryption key is not shared with

the server; and...

It should be understood that the object of the invention is to provide a method of distributing the location of the mobile device which safeguards the privacy of the user of the mobile device. The user of mobile device MS2 safeguards his privacy by only giving out the encryption key to certain parties (e.g., MS1) by attaching the encryption key to those communications issued from mobile device MS2 to the certain parties. In other words, if mobile device MS2 does not wish its location to be learned, it can protect its privacy by not attaching the encryption key to the communication.

The example scenario further discloses: Further suppose that a record relating to the location of telephone MS2 is maintained in the database held on the information server IS, the record including the number of the telephone MS2 and **an encrypted location of telephone MS2 previously determined and encrypted at telephone MS2 and uploaded to the database.**

These further steps are recited as the following elements of claim 1:

- the mobile device determining its location;
- the mobile device encrypting the determined location using a predetermined encryption key; and
- the mobile device uploading the determined encrypted location and a telephone number of the mobile device to a server for storage as a database record associated with the mobile device;
- the server storing the received encrypted location of the mobile device in the database record associated with the mobile device;

The example scenario further discloses – the user of telephone MS1 connects to the Internet using their mobile cellular telephone ...and accesses information server and queries the database held on the server by sending the telephone number of telephone MS2 to the information server. The information server replies sending the encrypted location.

These further steps are recited as the following elements of claim 1:

the remote terminal querying the database supported by the server by
sending the telephone number of the mobile device in response to receiving the
communication from the mobile device;
the server transmitting to the remote terminal the encrypted location of
the mobile device in response to the query;

The example scenario further discloses – upon receiving the encrypted location,
telephone MS1 decrypts the encrypted location of telephone MS2 using the encryption key
previously appended to the text message sent by telephone MS2.

These further steps are recited as the following element of claim 1:

...the remote terminal decrypting the encrypted location of the mobile
device using the predetermined encryption key received from the mobile
device.

It is respectfully submitted that neither Herle or Kempf teach the above recited
features of claim 1. The Examiner relies upon Herle's disclosure of querying the server from
a remote terminal. The Examiner points applicants to Herle, fig. 4, step 420, and col. 6, lines
48-50. However, the rejection is moot in light of Applicant's proposed amendments.

As stated above, applicants have amended the claim recitation to more clearly
and precisely recite that the remote terminal querying the database supported by the server by
sending the telephone number of the mobile device **in response to receiving the
communication from the mobile device**. The distinction being that the query is made in
response to receiving the communication from the mobile device, thereby involving three
parties, the server, the remote terminal and the mobile device, whereby the server merely
plays the role of storing encrypted location information and forwarding that information upon
request from the remote terminal, in response to receiving a communication from the mobile
device. In contrast to Applicant's amended claim recitation, Herle merely describes a two
party system whereby the MS location server 160 periodically or **aperiodically receive**

access requests from client access devices. (i.e., where an interaction involves the server and a single client). MS location server 160 authenticates the client access devices using user name and password verification procedures (process step 420).

Herle teaches @ col. 6, lines 48-50

MS location server 160 stores the encrypted MS 111 position data in a corresponding record in mobile station database 350 (process step 415). **Thereafter, MS location server 160 may periodically or aperiodically receive access requests from client access devices. MS location server 160 then authenticates the client access devices using user name and password verification procedures** (process step 420). In one embodiment of the present invention, if the client access device properly authenticates, MS location server 160 transmits the encrypted MS 111 position data to the client access device, which then decrypts the MS 111 position data. In an alternate embodiment of the present invention, MS location server 160 decrypts the MS 111 position data and transmits unencrypted MS 111 position data to authenticated client device (process step 425).

The Examiner cites Kempf for curing a deficiency in Herle. More particularly, Kempf is cited for teaching a step of attaching the encryption key to a communication between the mobile device and the remote terminal, wherein the encryption key is not shared with the server. However, Kempf suffers from the same deficiency as Herle, being a two party system. That is, neither reference teaches, taken alone or in any proper combination, using the shared encryption key between a first and second communicating party as a trigger for querying a third party (i.e., server) to request encrypted location information with which the encryption key may be used to decrypt and thereby ascertain the location of the first party. For all of the reasons noted above, independent claim 1 is submitted to clearly and patentably distinguish over the art of record.

Claim 2 is allowable

Regarding the rejection of claim 2, in the Office Action it is suggested that Herle teaches a step of sharing the predetermined encryption key with a remote terminal. Applicants respectfully disagree. The Examiner points Applicants to MS location server 160 – fig. 1, col. 6, lines 54-56 – transmitting the encrypted MS 111 position data to the client access device, which then decrypts the MS 111 position data; only mobile station and the remote terminal share encryption key in this embodiment of the invention. Applicants respectfully note that there is no teaching or suggestion of the mobile station and the remote terminal sharing the encryption key in a communication between the two entities. Rather, Herle discloses at col. 5,

lines 60-65 that the MS location server 160 **controls access to the location information from the mobile station**. Further, Herle at col. 6, lines 1-10 disclose that the MS position server application program 330 determines if the encryption/decryption key presented from a requesting entity can access the location information. Therefore, it is respectfully submitted that Herle does not teach at least a step of: *sharing the predetermined encryption key with a remote terminal by attaching the encryption key to a communication between the mobile device and the remote terminal, wherein the encryption key is not shared with the server*, as recited in claim 2. It has been shown that the encryption key is clearly shared with the server for the purpose of controlling access to the location information. This feature is in stark contrast to Applicant's method whereby the server merely acts as a data repository and freely supplies encrypted location information to requesting entities. Further, Kempf does not cure the deficiencies of Herle. For all of the reasons noted above, independent claim 1 is submitted to clearly and patentably distinguish over the art of record.

Claim 4 is allowable

Independent Claim 4 has been amended herein to better define Applicant's invention over the combination of Herle and Kempf. Claim 4 now recites limitations and/or features which are not disclosed by Herle or Kempf, taken alone and in any reasonable combination. Therefore, the cited portions of Herle and Kempf do not anticipate claim 4, because the cited portions of Herle and Kempf do not teach every element of claim 4. Claim 4 is reproduced below in clean form below. Claim 4 as amended now recites in relevant part, *receiving encrypted location information from the remote server in response to said query without authenticating the query*. Applicants contend that Herle requires that the access requests made from a client access device be authenticated in some manner. See, for example, claims 15, 19 and 20 of Herle (i.e., authenticating the access request for the geographic location information comprising one of determining if a password from the client device is authentic or determining if a decryption key is authentic).

4. A terminal configured to query a database supported by a remote server for the location of a particular mobile device in response to receiving a communication from the particular mobile device with which it has shared an encryption key

independently of the server via an attachment; receiving encrypted location information from the remote server in response to said query without authenticating the query; and upon receipt of an encrypted location encrypted with the encryption key, decrypting the location at the remote terminal, wherein said query includes at least a telephone number of the particular mobile device for use as an index into said database to identify said particular mobile device.

Further, Kempf does not cure the deficiencies of Herle. For all of the reasons noted above, independent claim 4 is submitted to clearly and patentably distinguish over the art of record.

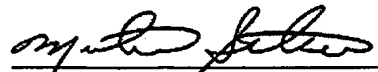
The amendments made herein are without prejudice to expedite prosecution at this time. Applicants expressly reserve the right to pursue the original claims and/or broader claims at another time.

Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims presently pending in the application, namely, Claims 1, 2 and 4 are believed to be in condition for allowance and patentably distinguishable over the art of record.

If the Examiner should have any questions concerning this communication or feels that an interview would be helpful, the Examiner is requested to call Mike Scaturro, Esq., Intellectual Property Counsel, Philips Electronics North America, at 516-414-2007.

Respectfully submitted,



Michael A. Scaturro
Reg. No. 51,356
Attorney for Applicants

Appl. No: ~~40/558,744~~ 10/535,327
Amendment and/or Response
Reply to Office action of 27 September 2010

Page 12 of 12

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, Previously Presented York 10510-8001